



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

APR 12 2001

MEMORANDUM FOR TREASURY INSPECTOR GENERAL FOR TAX
ADMINISTRATION

FROM:

John L. Zimmerman
John L. Zimmerman
Acting Chief Information Technology Services

SUBJECT

Response to Draft Audit Report: Employee's Extensive
Personal Use of the Internet Should Be Controlled

Attached is the IS management response for the above stated draft audit report. Included with the response is a copy of the memorandum signed by Bob Wenzel on November 8, 2000.

The management response to your findings and recommendations regarding the Internal Revenue Service (IRS) policy on employee use of the Internet was not originally submitted with the above mentioned memorandum.

If you have any questions regarding this management response, please feel free to contact me or a member of your staff may call Diane R. Robinson, Acting Office Manager, Program Oversight and Coordination, at (202) 283-4128.

Attachment

**Management Response to Draft Audit Report – Employees' Extensive
Personal Use of the Internet Should Be Controlled (Audit No. 200020030)**

RECOMMENDATION #1

The Chief Information Officer (CIO) should continue using the Internet blocking software and ensure the timely annual procurement of the software licensing agreement to receive timely updates to the blocking criteria starting with the year 2001.

ASSESSMENT OF CAUSE

When the audit was conducted, IRS was using a blocking software package; however, the subscription service was not renewed in a timely manner. That caused the IRS to miss some updates and that could have allowed sites to be accessed that would have otherwise been blocked.

CORRECTIVE ACTION

The CIO agrees with this recommendation and has renewed the Internet blocking software for Fiscal Year 2001.

IMPLEMENTATION DATE

Completed: October 2000

RESPONSIBLE OFFICIAL

Chief Information Technology Services
Deputy Chief Information Technology Services
Director, Telecommunications

MONITORING PLAN FOR CORRECTIVE ACTION #1

Not Applicable

**Management Response to Draft Audit Report – Employees' Extensive
Personal Use of the Internet Should Be Controlled (Audit No. 200020030)**

RECOMMENDATION #1

The Chief Information Officer (CIO) should continue using the Internet blocking software and ensure the timely annual procurement of the software licensing agreement to receive timely updates to the blocking criteria starting with the year 2001

ASSESSMENT OF CAUSE

When the audit was conducted, IRS was using a blocking software package; however, the subscription service was not renewed in a timely manner. That caused the IRS to miss some updates and that could have allowed sites to be accessed that would have otherwise been blocked.

CORRECTIVE ACTION

The CIO agrees with this recommendation and has renewed the Internet blocking software for Fiscal Year 2001.

IMPLEMENTATION DATE

Completed: October 2000

RESPONSIBLE OFFICIAL

Chief Information Technology Services
Deputy Chief Information Technology Services
Director, Telecommunications

MONITORING PLAN FOR CORRECTIVE ACTION #1

Not Applicable

Management Response to Draft Audit Report – Employees' Extensive Personal Use of the Internet Should Be Controlled (Audit No. 200020030)

RECOMMENDATION #2

The CIO should mandate that Internet-related activity logs from the IRS firewall and proxy servers are retained and periodically reviewed to identify inappropriate accesses.

ASSESSMENT OF CAUSE

Review of activity logs to determine employee use of the Internet was not in place during the period because of need to comply with a related Unfair Labor Practice (ULP) settlement. Furthermore, even if the ULP were not in place, it would be extremely difficult to review the logs for this purpose. The firewall and proxy servers generate log files that can be compiled and searched to determine which sites were visited and correlate that to a specific Internet Protocol (IP) address. Most of the Service uses Dynamic Host Configuration Protocol (DHCP) to assign IP addresses so each workstation is generally assigned an access upon use. The DHCP logs cannot tell what employee used a given IP address during an Internet session without a cumbersome process to match log on time with passwords.

The CIO agrees that monitoring of employee use of the Internet is a by-product of the recently negotiated IRS Internet Policy. However, the IRS is still considering which strategies will be used for this activity and subsequently, what role activity logs will play.

CORRECTIVE ACTION

The Office of Security is teamed with Telecommunications and TIGTA's Strategic Enforcement Division in the Incident Response Center. Guidelines are currently being established for accountability, roles, and responsibilities. This includes actions that result when incidents occur during routine monitoring of intrusion detection systems or firewalls.

IMPLEMENTATION DATES

Proposed: November 1, 2001

RESPONSIBLE OFFICIAL

Chief Information Technology Services
Director Office of Security

MONITORING PLAN FOR CORRECTIVE ACTIONS

Not Applicable

**Management Response to Draft Audit Report – Employees' Extensive
Personal Use of the Internet Should Be Controlled (Audit No. 200020030)**

RECOMMENDATION #3

The CIO should augment the vendor's blocking criteria list with known inappropriate sites identified during monitoring efforts or from referrals. Based on our review, external streaming video web sites should be blocked from employee access until the IRS Telecommunications Branch can fully evaluate its impact on bandwidth and ensure its use will not hinder other business telecommunications traffic.

ASSESSMENT OF CAUSE

The IRS uses a blocking software product to restrict access to sites containing materials not deemed appropriate for business use of the Internet. The software is updated weekly. Additionally, the IS staff has not conducted any specific modeling or projections to assess the impact of any expanded use of the Internet non-business purposes to support taking action to allow such use by employees.

CORRECTIVE ACTIONS

- 3a. The IS organization will assess other products that might offer more options to blocking sites than are currently available in the WebNot software. IS will implement such products upon review and approval of IS executive management.
- 3b. The IS organization will assess products and tools to block video and audio streaming capabilities to the Internet. IS will implement such products upon review and approval of IS executive management. Once blocked, the reactivation of video or audio streaming will only be done as a result of documented business needs approved in the IRS Strategic Plan process.

IMPLEMENTATION DATES

- 3a. Proposed: June 2001
- 3b. Proposed: May 2001

RESPONSIBLE OFFICIAL

Chief Information Technology Services
Deputy Chief Information Technology Services
Director, Telecommunications

MONITORING PLAN FOR CORRECTIVE ACTIONS

- 3a: Not Applicable
- 3b: Not Applicable

**Management Response to Draft Audit Report – Employees’ Extensive
Personal Use of the Internet Should Be Controlled (Audit No. 200020030)**

RECOMMENDATION #4

The CIO should consider the impact on IRS resources prior to deciding to implement a “limited personal use” Internet policy.

ASSESSMENT OF CAUSE

When Internet access was introduced on the end user workstation, there was little demand for bandwidth. As uses have grown for conducting training, service ordering, and other applications, so has the need for available bandwidth.

CORRECTIVE ACTIONS

- 4a. The CIO will perform appropriate traffic analysis relative to expanding Internet access for personal use before any recommendation is made whether or not to change the IRS Internet policy to allow for non-business use.
- 4b. The CIO will perform appropriate cost estimates relative to expanding Internet access for personal use before any recommendation is made whether or not to change the IRS Internet policy to allow for non-business use.
- 4c. The CIO will recommend a policy on non-business use of the Internet.
- 4d. Implement IRS policy changes on non-business use of the Internet.

IMPLEMENTATION DATES

- 4a. Proposed: July 1, 2001
- 4b. Proposed: September 1, 2001
- 4c. Proposed: October 1, 2001
- 4d. Proposed: November 1, 2001

RESPONSIBLE OFFICIAL

Chief Information Technology Services
Deputy Chief Information Technology Services
Director, Telecommunications

MONITORING PLAN FOR CORRECTIVE ACTIONS

- 4a: Not Applicable
- 4b: Not Applicable
- 4c: Secure Commissioner’s signature on policy on non-business use of Internet
- 4d: Disseminate policy to all IRS employees